IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSON

LORI BUSCHER, individually, and on behalf of all others similarly situated, Plaintiff, v. ALTA RESOURCES CORP., Defendant.	Case No. _____ **CLASS REPRESENTATION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Lori Buscher ("Plaintiff"), individually, and on behalf of all others similarly situated, brings this action against Alta Resources Corp. ("Alta Resources" or "Defendant"). Plaintiff brings this action by and through her attorneys, and allege, based upon personal knowledge as to their own actions, and based upon information and belief and reasonable investigation by their counsel as to all other matters, as follows.

I. INTRODUCTION

1. Alta Resources provides shipping, sales, customer management, fundraising, and marketing services for companies based in the United States and Latin America. Alta Resources has offices across North America, South America, and Asia.

2. As part of its operations, Alta Resources collects, maintains, and stores highly sensitive personal and medical information belonging to its employees, customers, and marketing targets, including, but not limited to their full names, Social Security numbers, dates of birth, addresses, driver's license numbers (collectively, "personally identifying information" or "PII"), information regarding medical treatment, diagnosis, and prescriptions, medical record numbers, health insurance information, and other protected health information (collectively, "private health

information" or "PHI"), as well as financial account/payment card information ("financial account information") (collectively, "Private Information").

3. On November 17, 2024, Alta Resources experienced a data breach incident in which unauthorized cybercriminals accessed its information systems and databases and accessed Private Information belonging to Plaintiff and Class members (the "Data Breach"). Alta Resources discovered this unauthorized access on November 18, 2024. Subsequent investigation by Alta Resources determined that the unauthorized actors were able to access Private Information concerning Plaintiff and Class members.

4. On December 20, 2024, Alta Resources sent a notice to individuals whose information was accessed in the Data Breach.

5. Because Alta Resources stored and handled Plaintiff's and Class members' highly-sensitive Private Information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

6. Ultimately, Alta Resources failed to fulfill this obligation, as unauthorized cybercriminals breached Alta Resources's information systems and databases and stole vast quantities of Private Information belonging to Alta Resources's customers, employees, and marketing targets, including Plaintiff and Class members. The Data Breach were the direct, proximate, and foreseeable results of multiple failings on the part of Alta Resources.

7. The Data Breach occurred because Alta Resources failed to implement reasonable security protections to safeguard its information systems and databases. Moreover, before the Data Breach occurred, Alta Resources failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and Class members been made aware of this fact, they would have never provided such information to Alta Resources.

8. Alta Resources's subsequent handling of the breach was also deficient.

9. Alta Resources unreasonably delayed for one month before it began informing victims of the Data Breach. Furthermore, Alta Resources's meager attempt to ameliorate the effects of this data breach with one year of credit monitoring years of complimentary credit monitoring is woefully inadequate. Much of the Private Information that was stolen is immutable and one year of credit monitoring is nothing in the face of a life-long heightened risk of identity theft.

10. As a result of Alta Resources's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff and Class members suffered injuries, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;
- Charges and fees associated with fraudulent charges on their accounts; and
- The continued and increased risk of compromise to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

11. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief for the consequences of Defendant's failure to reasonably safeguard Plaintiff's and

Class members' Private Information; its failure to reasonably provide timely notification to Plaintiff and Class members that their Private Information had been compromised; and for Defendant's failure to inform Plaintiff and Class members concerning the status, safety, location, access, and protection of their Private Information.

II. PARTIES

Plaintiff Lori Buscher

12. Plaintiff Lori Buscher is a resident and citizen of Oshkosh, Wisconsin. Plaintiff Buscher was an employee of Alta Resources. Plaintiff Buscher received Defendant's Data Breach Notice.

Defendant Alta Resources Corp.

13. The Alta Resources is a Wisconsin corporation with its principal place of business located at Neenah, Wisconsin. Defendant conducts business in this District and throughout Wisconsin.

III. JURISDICTION AND VENUE

14. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

15. This Court has personal jurisdiction over Defendant because Defendant is headquartered in Wisconsin.

16. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District and because Defendant resides in this District.

IV. FACTUAL ALLEGATIONS

A. Alta Resources – Background

17. Alta Resources is provides shipping, sales, customer management, fundraising, and marketing services for companies based in the United States and Latin America. As part of its normal operations, Alta Resources collects, maintains, and stores large volumes of Private Information belonging to its current and former customers, employees, and marketing targets.

18. Alta Resources failed to implement necessary data security safeguards at the time of the Data Breach. This failure resulted in cybercriminals accessing the Private Information of Alta Resources's current and former employees, customers, and marketing targets—Plaintiff and Class members.

19. Current and former employees and customers of Alta Resources, such as Plaintiff and Class members, made their Private Information available to Alta Resources with the reasonable expectation that any entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. They similarly expected that, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

20. This expectation was objectively reasonable and based on an obligation imposed on Alta Resources by statute, regulations, industrial custom, and standards of general due care.

21. Unfortunately for Plaintiff and Class members, Alta Resources failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result,

it failed to protect Plaintiff and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

22. According to Defendant's public statements, cybercriminals breached Alta Resources's information systems on or about November 17, 2024 through November 18, 2024. On November 18, 2024, Alta Resources discovered the Data Breach.

23. On December 20, 2024, Alta Resources sent notice of the Data Breach to all individuals affected by this data security incident.

24. Omitted from the notice were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

25. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class members of the Data Breach's critical facts. Without these details, Plaintiff's and Class members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

26. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

27. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class members. Plaintiff's and Class members' Private Information was accessed and stolen in the Data Breach.

28. Plaintiff further believes that her Private Information and that of Class members was or will be sold on the dark web, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type

29. Alta Resources estimates that the Private Information belonging to at least 37,000 individuals was compromised in this incident.

C. Alta Resources' Many Failures Both Prior to and Following the Breach

30. Defendant collects and maintains vast quantities of Private Information belonging to Plaintiff and Class members as part of its normal operations. The Data Breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendant.

31. First, Defendant inexcusably failed to implement reasonable security protections to safeguard its information systems and databases.

32. Second, Defendant failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and Class members been aware that Defendant did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to Defendant.

33. In addition to the failures that lead to the successful breach, Defendant's failings in handling the breach and responding to the incident exacerbated the resulting harm to the Plaintiff and Class members.

34. Defendant's delay in informing victims of the Data Breach that their Private Information was compromised virtually ensured that the cybercriminals who stole this Private Information could monetize, misuse and/or disseminate that Private Information before the Plaintiff and Class members could take affirmative steps to protect their sensitive information. As

a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

35. Additionally, Defendant's attempt to ameliorate the effects of this Data Breach with limited complimentary credit monitoring is woefully inadequate. Plaintiff's and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. As a consequence, they face the real, immediate, and likely danger of identity theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the stolen Private Information, such as healthcare data, is immutable.

36. In short, Defendant's myriad failures, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiff's and Class members' Private Information for one month before Defendant finally granted victims the opportunity to take proactive steps to defend herself and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

37. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, and Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

38. The Identity Theft Resource Center's ("ITRC") Annual End-of-Year Data Breach Report for 2023 listed 3,205 total compromises involving 353,027,892 victims.[1] This is nearly double the number of compromises in 2022, which had 1,802 total compromises involving

[1] *2023 Data Breach Report*, Identity Theft Resource Center (January 2023), available at https://www.idtheftcenter.org/publication/2023-data-breach-report/.

422,143,312 victims.[2] The 2022 figure was itself just 50 compromises short of the then record-breaking total of 1,852 set in 2021.[3] As it stands, the number of compromises in 2023 has managed to shatter 2021's record by a factor of 2.

39. The HIPAA Journal's 2023 Health Care Data Breach Report noted 725 data breaches involving 500 or more healthcare records.[4] In 2022, there were 707 compromises involving healthcare data in 2022 and 715 in 2021.[5]

40. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 3,205 in 2023.[6] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 353 million in 2023.[7]

---

[2] *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report.
[3] *Id.*
[4] Steve Adler, December 2023 Healthcare Data Breach Report, The HIPAA Journal (January 18, 2024), available at https://www.hipaajournal.com/december-2023-healthcare-data-breach-report/.
[5] *2022 Healthcare Data Breach Report*, The HIPAA Journal (January 24, 2023), available at: https://www.hipaajournal.com/2022-healthcare-data-breach-report/.
[6] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2023*, Statista (Nov 9, 2024), available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed.
[7] *Id.*

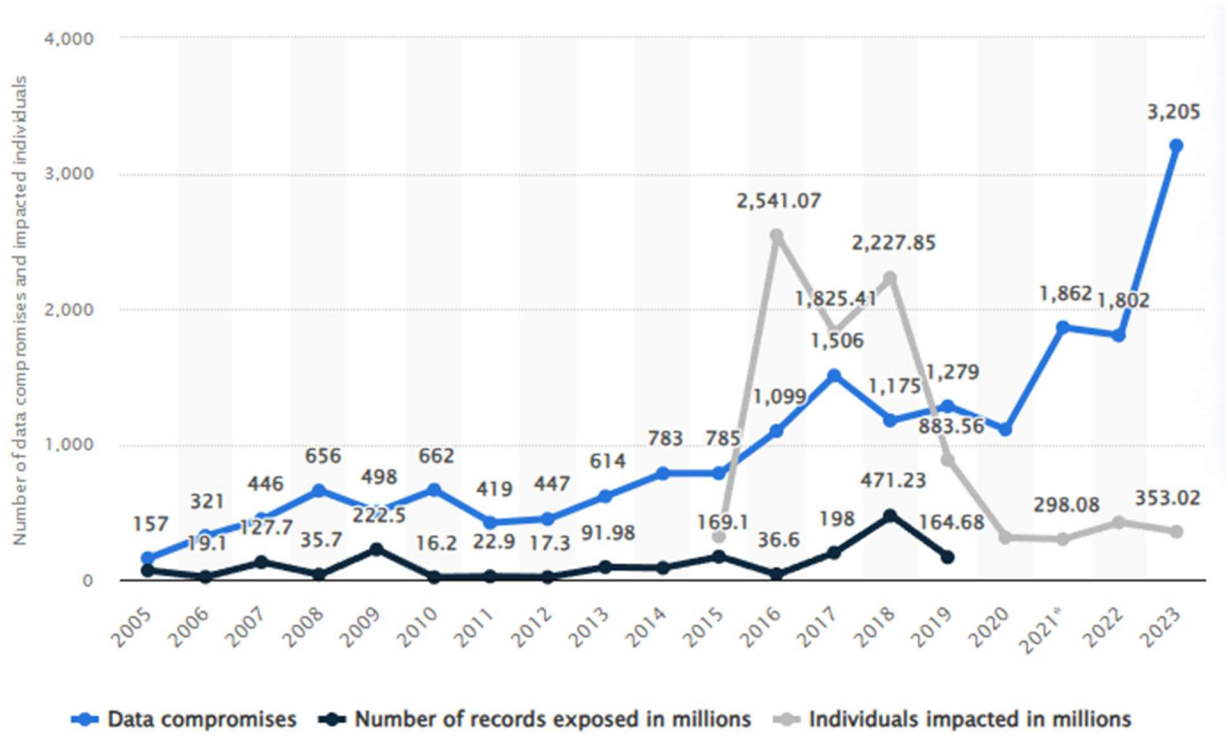

Figure 1 –*Number of Data Breaches and Affected Individuals from 2005 to 2023.* [8]

41. This stolen PII is then routinely traded on dark web black markets as a simple commodity, with online banking login information costing an average of $100, full credit card details and associated details costing between $10 and $100, and comprehensive data packages enabling complete identity theft selling for $1,000.[9]

42. In addition, the severity of the consequences of a compromised Social Security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory groups can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> [a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your

[8] *Id.*
[9] Ryan Smith, *Revealed-how much is personal information worth on the dark web?*, Insurance News (May 1, 2023), available at https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx.

> good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[10]

This is exacerbated by the fact that the problems arising from a compromised Social Security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[11]

43. Further, as data breaches become ever more prevalent and as technology advances, computer programs can scan the internet to create a mosaic of information that could be used to link compromised information to an individual in ways in a phenomenon known as the "mosaic effect." By and through this process, names, dates of birth, and contact information such as telephone numbers and email addresses, hackers and identity thieves can access users' other accounts by, for example, bypassing security questions and 2FA security with the comprehensive collection of information at their disposal.

44. Thus, because of this effect, cybercriminals and other unauthorized parties could use Plaintiff's and Class Members' Private Information to access, inter alia, email accounts and

[10] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.
[11] *Id.*

financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members, even when that specific category of information is not compromised in a given breach.

45. A particularly trouble example of this effect is the development of "Fullz" packages. A "Fullz" packages is a dosser of information that cybercriminals and other unauthorized parties can assemble by cross-referencing the Private Information compromised in a given data breach to publicly available data or data compromised in other data breaches. Automated programs can and are routinely used to create these dossiers and they typically represent an alarmingly accurate and complete profile of a given individual.

46. Therefore, through the use of these "Fullz" packages, stolen Private Information from this Data Breach can be easily linked to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. Thus, even if certain information such as emails, phone numbers, or credit card or financial account were not compromised in this Data Breach, criminals can easily create a Fullz package to sell for profit.

47. Upon information and belief, this has already transpired (and will continue to transpire) for Plaintiff and the Class. And any reasonable for any trier of fact will find that Plaintiff and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

48. The most sought after and expensive information on the dark web are stolen medical records which command prices from $250 to $1,000 each.[12] Medical records are considered the most valuable because unlike credit cards, which can easily be canceled, and Social Security numbers, which can be changed, medical records contain "a treasure trove of unalterable

[12] Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (January 26, 2021), available at: https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.

data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[13] With this bounty of ill-gotten information, cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.[14] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.[15] Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.[16]

49. The wrongful use of compromised medical information is known as medical identity theft and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of $13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[17] It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.[18]

---

[13] *Id.*
[14] *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), available at https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare. *See also* Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (August 25, 2016), available at https://www.consumerreports.org/health/medical-identity-theft-a1699327549/; *Data Breaches: In the Healthcare Sector*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited December 1, 2024).
[15] *Id.*
[16] *Id.*
[17] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.
[18] *Id.*

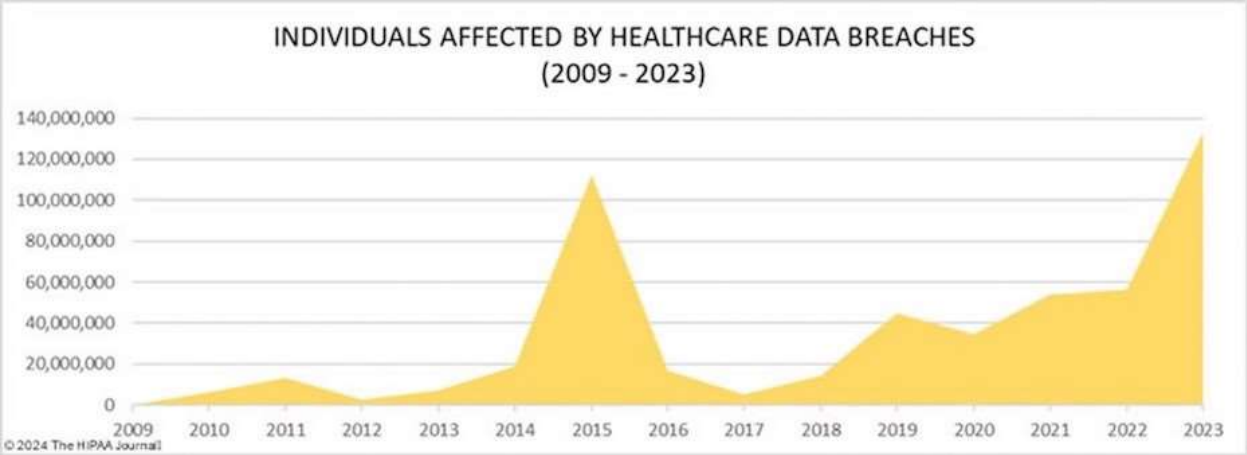

Figure 2 –*Number of Individuals Affected by Healthcare Data Breaches from 2009 to 2023.*[19]

50. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Defendant charged with maintaining and securing customer and employee PII should know the importance of protecting that information from unauthorized disclosure. Indeed, Defendant knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[20]

51. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized

[19] *Healthcare fraud and the burden of medical ID theft*, Experian Health (February 14, 2024), available at https://www.experian.com/blogs/healthcare/healthcare-fraud-and-the-burden-of-medical-id-theft.
[20] *See, e.g.*, Steve Adler, *Healthcare Data Breach Statistics*, HIPAA Journal (November 25, 2024), available at: https://www.hipaajournal.com/healthcare-data-breach-statistics.

these enforcement actions to place companies like Defendant on notice of their obligation to safeguard employee and customer information.[21]

52. Given the nature of Defendant's Data Breach, as well as the length of the time Defendant's networks were breached and the long delay in notification to victims thereof, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class members' Private Information can easily obtain Plaintiff's and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[22] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

54. To date, Defendant has offered its consumers only limited identity theft monitoring services. The services offered are inadequate to protect Plaintiff and Class members from the threats they will face for years to come, particularly in light of the Private Information at issue here.

55. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own

[21] *See, e.g.*, *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).
[22] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1. *See also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/.

acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from misappropriation. As a result, the injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for its current and former employees and customers.

E. Alta Resources Had a Duty and Obligation to Protect Private Information

56. Defendant has an obligation to protect the Private Information belonging to Plaintiff and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and medical records. Third, Defendant imposed such an obligation on itself with its promises regarding the safe handling of data. Plaintiff and Class members provided, and Defendant obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. HIPAA Requirements and Violation

57. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

58. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . . ." 45 CFR § 164.402.

59. Defendant failed to implement and/or maintain procedures, systems, and safeguards to protect the Private Information belonging to Plaintiff and Class members from unauthorized access and disclosure.

60. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

61. Upon information and belief, Defendant also failed to store the information it collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

2. FTC Act Requirements and Violations

62. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

63. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[23] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[24] The guidelines also recommend that businesses

[23] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed August 15, 2023).
[24] *Id.*

use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[25] Defendant clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data accessed.

64. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

65. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

67. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

[25] *Id.*

68. Defendant was fully aware of its obligation to protect the Private Information of its current and former employees and customers, including Plaintiff and Class members. Defendant is a sophisticated and technologically savvy business that relies extensively on technology systems and networks to maintain its practice, including storing its customers' and employees' PII, protected health information, and medical information in order to operate its business.

69. Defendant had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and Plaintiff and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' Private Information.

3. Industry Standards and Noncompliance

70. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

71. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information, like Defendant, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

72. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports;

protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

73. Defendant should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

74. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

4. Defendant's Own Stated Policies and Promises

75. Defendant's own published privacy policy states that: "At Alta we have set a high standard for securing our customers' data and our clients' peace of mind. Operating in a changed world of highly sensitive personal information and privacy concerns, we have best practices rooted in system integrity, security and auditing compliance. We currently foster a S.A.F.E. environment that complies with multiple agencies, such as the FDA, HIPAA and more."[26] Alta Resources claims that they "have joined the ranks of the securest of the secure."

76. Defendant failed to live up to its own stated policies and promises with regards to data privacy and data security as cybercriminals were able to infiltrate its systems and steal the Private Information belonging to Plaintiff and Class members.

[26] Alta Resources, "Security," https://www.altaresources.com/security/.

F. Plaintiff and the Class Suffered Harm Resulting from the Data Breach

77. Like any data hack, the Data Breach presents major problems for all affected.[27]

78. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[28]

79. The ramifications of Defendant's failure to properly secure Plaintiff's and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

80. According to data security experts, one out of every four data breach notification recipients become a victim of identity fraud.

81. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

82. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal *Preventive Medicine Reports*, public and corporate data breaches correlate to an

[27] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.
[28] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

increased risk of identity theft for victimized consumers.[29] The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[30]

83. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

84. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being $4.45 million dollars in 2023.[31] The average cost to resolve a data breach involving health information, however, is more than double this figure at $10.92 million.[32]

85. The theft of medical information, beyond the theft of more traditional forms off PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years and this explosive growth far outstrips the increase in incidence of traditional identity theft.[33] Medical Identity Theft is especially nasty for victims because of the lack of laws that limit a victim's liabilities and damages from this type of identity theft (e.g., a victim's liability for fraudulent credit card charges is capped at $50),

---

[29] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.
[30] *Id.*
[31] *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds.
[32] *Id.*
[33] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.

the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average, $13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.[34]

86. In response to the Data Breach, Defendant offered to provide certain individuals whose Private Information was exposed in the Data Breach with one year of credit monitoring. However, this is inadequate to protect victims of the Data Breach from the lifelong risk of harm imposed on them by Defendant's failures.

87. Moreover, the credit monitoring offered by Defendant is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access of their sensitive Private Information.

88. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with time spent to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they

[34] *Id.*

were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiff's and Class members' privacy.

89. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will not abate within the limited time of credit monitoring offered by Defendant.

90. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure Private Information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and they have incurred and will incur actual damages in an attempt to prevent identity theft.

91. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both herself and similarly situated individuals whose Private Information was accessed in the Data Breach.

G. EXPERIENCES SPECIFIC TO PLAINTIFF

Lori Buscher

92. Plaintiff Lori Buscher is a former employee of Alta Resources.

93. Plaintiff Buscher received Alta Resources's data breach notice. The notice informed Plaintiff Buscher that her Private Information was improperly accessed and obtained by third parties.

94. After the breach, Plaintiff Buscher has experienced an increase in unsolicited phone calls, emails, and text messages.

95. As a result of the Data Breach, Plaintiff Buscher has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Buscher has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

96. As a result of the Data Breach, Plaintiff Buscher has suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her Private Information for purposes of identity theft and fraud. Plaintiff Buscher is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

97. Plaintiff Buscher suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

98. As a result of the Data Breach, Buscher anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS REPRESENTATION ALLEGATIONS

99. Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose Private Information was accessed in the Data Breach.

Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

100. In the alternative, Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

> All persons who are residents of the State of Wisconsin whose Private Information was accessed in the Data Breach (the "Wisconsin Subclass").

Excluded from the Subclass are Defendant, its executives and officers, and the Judge(s) assigned to this case.

101. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiff only through the discovery process. On information and belief, the number of affected individuals estimated to be 37,000.[35] The members of the Class will be identifiable through information and records in Defendant's possession, custody, and control.

102. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over

[35] Maine Attorney General, "Data Breach Notifications," https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/0e914ae8-3620-4369-8169-4fd1a562ca27.html

the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When Defendant learned of the Data Breach;

b. Whether hackers obtained Class members' Private Information via the Data Breach;

c. Whether Defendant's response to the Data Breach was adequate;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

f. Whether Defendant owed a duty to safeguard their Private Information;

g. Whether Defendant breached its duty to safeguard Private Information;

h. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

i. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

j. Whether Defendant's conduct violated the FTCA, HIPAA, and/or the Consumer Protection Act invoked herein;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct was *per se* negligent;

m. Whether Defendant was unjustly enriched;

n. What damages Plaintiff and Class members suffered as a result of Defendant's misconduct;

o. Whether Plaintiff and Class members are entitled to actual and/or statutory damages; and

p. Whether Plaintiff and Class members are entitled to additional credit or identity monitoring and monetary relief.

103. Typicality: Plaintiff's claims are typical of the claims of the Class as Plaintiff and all members of the Class had their Private Information compromised in the Data Breach. Plaintiff's claims and damages are also typical of the Class because they resulted from Defendant's uniform wrongful conduct. Likewise, the relief to which Plaintiff is entitled to is typical of the Class because Defendant has acted, and refused to act, on grounds generally applicable to the Class.

104. Adequacy: Plaintiff is adequate class representatives because her interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, they have retained counsel competent and highly experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor her counsel have any interests that are antagonistic to the interests of other members of the Class.

105. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class, a class action is superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(By Plaintiff on behalf of the Class)

106. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

107. Defendant owes a duty of care to protect the Private Information belonging to Plaintiff and Class members. Defendant also owes several specific duties including, but not limited to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect employee and customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;

d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class members pursuant to the FTCA;

e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. to promptly notify Plaintiff and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

108. Defendant owes this duty because it had a special relationship with Plaintiff and Class members. Plaintiff and Class members entrusted their Private Information to Defendant on the understanding that adequate security precautions would be taken to protect this information. Furthermore, only Defendant had the ability to protect its systems and the Private Information stored on them from attack.

109. Defendant also owes this duty because industry standards mandate that Defendant protect its employees and employees' confidential Private Information.

110. Defendant also owes a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiff and Class members. This duty exists to provide Plaintiff and Class members with the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

111. Defendant breached its duties owed to Plaintiff and Class members by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard their Private Information.

112. Defendant also breached the duties it owed to Plaintiff and Class members by failing to timely and accurately disclose to them that their Private Information had been improperly acquired and/or accessed.

113. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; and
- Permanent increased risk of identity theft.

114. Plaintiff and Class members were foreseeable victims of any inadequate security practices on the part of Defendant and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

115. In failing to provide prompt and adequate individual notice of the Data Breach, Defendant also acted with reckless disregard for the rights of Plaintiff and Class members.

116. Plaintiff is entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT II
NEGLIGENCE *PER SE*
(By Plaintiff on behalf of the Class)

117. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

118. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, imposes a duty on Defendant to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiff and Class members.

119. HIPAA imposes a duty on Defendant to implement reasonable safeguards to protect Plaintiff's and Class members' Private Information. 42 U.S.C. § 1302(d), *et seq*.

120. HIPAA also requires Defendant to render unusable, unreadable, or indecipherable all Private Information it collected. Defendant was required to do so through "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

121. Defendant violated the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiff's and Class members' Private Information.

122. Defendant violated HIPAA by failing to properly encrypt the Private Information it collected.

123. Defendant's failure to comply with HIPAA and the FTCA constitutes negligence *per se*.

124. Plaintiff and Class members are within the class of persons that the FTCA and HIPAA are intended to protect.

125. It was reasonably foreseeable that the failure to protect and secure Plaintiff's and Class members' Private Information in compliance with applicable laws and industry standards would result in that Information being accessed and stolen by unauthorized actors.

126. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to theft of their personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased risk of identity theft.

127. Plaintiff and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT III
BREACH OF IMPLIED CONTRACT
(By Plaintiff on behalf of the Class)

128. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

129. Plaintiff and Class members provided Defendant with their Private Information.

130. By providing their Private Information, and upon Defendant's acceptance of this information, Plaintiff and the Class, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

131. The implied contracts between Defendant and Plaintiff and Class members obligated Defendant to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' Private Information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. Defendant expressly adopted and assented to these terms in its public statements, representations and promises as described above.

132. The implied contracts for data security also obligated Defendant to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information.

133. Defendant breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' Private Information; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

134. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and Class members have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information, and are entitled to damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(By Plaintiff on behalf of the Class)

135. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

136. This count is brought in the alternative to Count III.

137. Plaintiff and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Defendant.

138. Plaintiff and the Class conferred their Private Information to Defendant as part of receiving medical care, employment and employment benefits, and other services. The Class also conferred payment to Defendant in exchange for medical services.

139. Plaintiff and Class members conferred their Private Information alongside payment with the understanding that the payment was, in part, to be used to implement data security sufficient to adequately protect their Private Information. And this payment represented a benefit that was to be used for a specific purpose.

140. Defendant, as a company collecting marketing, health insurance, and financial information, received payment from its customers to handle and manage this Private Information. Plaintiff and Class members conferral of their Private Information was a direct benefit since Defendant was able to use this information for business purposes and financial gain. There was an understanding that a portion of the monies Defendant received from the use of this Private Information, was intended to be used to implement data security sufficient to adequately protect this Private Information.

141. Defendant understood that it was so benefitted.

142. However, instead of providing a reasonable level of security, training, protocols, and other measures that would have prevented the Data Breach, as described in detail above,

Defendant, upon information and belief, knowingly and opportunistically elected to increase its own profits at the expense of Plaintiff and Class members by not expending the money required to do so.

143. And in failing to expend the monies conferred with the express understanding that it would be used on data security, Defendant knowingly and deliberately enriched itself at the expense of Plaintiff and Class members.

144. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and Class members in an unfair and unconscionable manner.

145. Defendant is therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically the value to Defendant of the Private Information that was accessed in the Data Breach and the profits Defendant received from the use and sale of that information. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

COUNT V
BREACH OF FIDUCIARY DUTY
(By Plaintiff on behalf of the Class)

146. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

147. Plaintiff brings this claim on behalf of herself and the Class.

148. Plaintiff and Class members provided their Private Information to Defendant in confidence with the reasonable belief that Defendant would protect their information. Plaintiff and

Class members would not have provided their information to Defendant had they known it would fail to adequately protect their information.

149. In collecting and maintaining this Private Information, Defendant created a fiduciary relationship between it and Plaintiff and Class members. As such, Defendant owed a duty to *primarily* act for the benefit of its current and former employees and customers upon matters within the scope of their relationship. This included a duty to protect Plaintiff's and Class Members' Private Information.

150. These fiduciary duties and responsibilities are also described under the procedures set forth in the HIPAA Privacy Rule, including the procedures and definitions found in 45 C.F.R. §160.103 and 45 C.F.R. §164.530, which requires Defendant to apply appropriate administrative, technical, and physical safeguards to protect the privacy of employee and customer information and to secure the health care information it maintains and to keep it free from disclosure.

151. Defendant breached these fiduciary duties by failing to implement adequate safeguards and causing Plaintiff's and Class members' Private Information to be disclosed to unauthorized third parties. Defendant further breached these fiduciary duties by contracting or otherwise doing business with companies that similarly failed to implement adequate safeguards, and sharing Plaintiff and Class members' Private Information with these entities.

152. As a direct and proximate result of Defendant's breaches of its fiduciary duties and the resulting disclosure of Plaintiff and Class member's Private Information, Plaintiff and Class members have suffered damages, including, but not limited to exposure to heightened future risk of identity theft, loss of privacy, confidentiality, and emotional distress.

COUNT VI
INVASION OF PRIVACY
(By Plaintiff on behalf of the Class)

153. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

154. Plaintiff and Class members had a reasonable expectation of privacy in the Private Information that Defendant possessed and/or continues to possess.

155. By failing to keep Plaintiff's and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Defendant invaded Plaintiff's and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiff and Class members, which is highly offensive to a reasonable person.

156. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider Defendant's actions highly offensive.

157. Defendant invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

158. As a proximate result of such misuse and disclosures, Plaintiff and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

159. In failing to protect Plaintiff's and Class members' Private Information, and in misusing and/or disclosing their Private Information, Defendant has acted with malice and oppression and in conscious disregard of Plaintiff's and Class members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its

own economic, corporate, and legal interests above the privacy interests of its thousands of customers and employees. Plaintiff, therefore, seeks an award of damages, including punitive damages, on behalf of herself and the Class.

COUNT VII
VIOLATIONS OF WISCONSIN'S DECPTIVE TRADE PRACTICES ACT
Wis. Stat. § 100.18
(By Plaintiff on behalf of the Wisconsin Subclass)

160. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

161. Plaintiff is authorized to bring this claim under Wisconsin Statute Section 100.18, which prohibits any "statement or representation contains any assertion, representation or statement of fact which is untrue, deceptive or misleading." Wis. Stat. § 100.18.

162. As described in this Complaint, Defendant has engaged in the following unfair or deceptive acts or practices in violation of the Wisconsin Deceptive Trade Practices Act: Substituting "services of inferior value or quality for the property or services which must be purchased."

163. Defendant's deceptive practices include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information; and

h. Failing to promptly and adequately notify Plaintiff and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

164. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant's relevant acts, practices, and omissions complained of in this action were done in the course of Defendant's business of marketing, offering for sale, and selling goods and services to consumers throughout the United States.

165. Defendant had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiff's and Class members' Private Information. This exclusive knowledge includes, but is not limited to, information that Defendant received through internal and other non-public audits and reviews that concluded that Defendant's security policies were substandard and deficient, and that Plaintiff's and Class members' Private Information and other Defendant data was vulnerable.

166. Defendant had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

167. Defendant also had exclusive knowledge about the length of time that it maintained individuals' Private Information after they stopped using services that necessitated the transfer of that Private Information to Defendant.

168. Defendant failed to disclose, and actively concealed, the material information it had regarding Defendant's deficient security policies and practices and regarding the security of the sensitive Private Information. For example, even though Defendant has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiff's and Class members' Private Information was vulnerable as a result, Defendant failed to disclose this information to, and actively concealed this information from, Plaintiff, Class members and the public. Defendant also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains Private Information and other records.

169. Likewise, during the days and weeks following the Data Breach, Defendant failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

170. Defendant had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, and because Defendant was in a fiduciary position by virtue of the fact that Defendant collected and maintained Plaintiff's and Class members' Private Information.

171. Defendant's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and its ability to protect the confidentiality of current and former employees', contractors', customers', and others' Private Information.

172. Had Defendant disclosed to Plaintiff and the Class that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class members' Private Information without advising that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their Private Information.

173. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

174. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws such as the FTC Act.

175. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to consumers or to competition and are not injuries that Plaintiff and the Class should have reasonably avoided.

176. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct result of Defendant's deceptive acts and practices as set forth herein include, without limitation: (i) Plaintiff experiencing an increase in spam calls, texts, and/or emails; (ii) invasion of privacy; (iii) theft of their Private Information; (vi) lost or diminished value of Private Information; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) loss of benefit of the bargain; (ix) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties

to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Private Information from a foreseeable and preventable cyber-attack.

177. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is proper class representatives; and appoint Plaintiff's Counsel as Class Counsel;

B. That Plaintiff be granted the declaratory relief sought herein;

C. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

D. That the Court award Plaintiff and Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiff and Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the putative Class, demand a trial by jury on all issues so triable.

Date: January 2, 2024

Respectfully Submitted,

/s/ Nickolas J. Hagman
Daniel O. Herrera*
Nickolas J. Hagman
Nabihah Maqbool*
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

* *Pro Hac Vice* forthcoming

Attorneys for Plaintiff and the Proposed Class